

Protocolo TCP/IP

La suite TCP/IP

Internet es un conglomerado muy amplio y extenso en el que se encuentran ordenadores con sistemas operativos incompatibles, redes más pequeñas y distintos servicios con su propio conjunto de protocolos para la comunicación. Ante tanta diversidad resulta necesario establecer un conjunto de reglas comunes para la comunicación entre estos diferentes elementos y que además optimice la utilización de recursos tan distantes. Este papel lo tiene el protocolo TCP/IP. TCP/IP también puede usarse como protocolo de comunicación en las redes privadas intranet y extranet.


Las siglas TCP/IP se refieren a dos protocolos de red, que son *Transmission Control Protocol* (Protocolo de Control de Transmisión) e *Internet Protocol* (Protocolo de Internet) respectivamente. Estos protocolos pertenecen a un conjunto mayor de protocolos. Dicho conjunto se denomina *suite TCP/IP*.


Los diferentes protocolos de la suite TCP/IP trabajan conjuntamente para proporcionar el transporte de datos dentro de Internet (o Intranet). En otras palabras, hacen posible que accedamos a los distintos servicios de la Red. Estos servicios incluyen, como se comentó en el capítulo 1: transmisión de correo electrónico, transferencia de ficheros, grupos de noticias, acceso a la World Wide Web, etc.

Hay dos clases de protocolos dentro de la suite TCP/IP que son: *protocolos a nivel de red* y *protocolos a nivel de aplicación*.

Protocolos a Nivel de Red

Estos protocolos se encargan de controlar los mecanismos de transferencia de datos. Normalmente son invisibles para el usuario y operan por debajo de la superficie del sistema. Dentro de estos protocolos tenemos:

 **TCP.** Controla la división de la información en unidades individuales de datos (llamadas paquetes) para que estos paquetes sean encaminados de la forma más eficiente hacia su punto de destino. En dicho punto, TCP se encargará de reensamblar dichos paquetes para reconstruir el fichero o mensaje que se envió. Por ejemplo, cuando se nos envía un fichero HTML desde un servidor Web, el protocolo de control de transmisión en ese servidor divide el fichero en uno o más paquetes, numera dichos paquetes y se los pasa al protocolo IP. Aunque cada paquete tenga la misma dirección IP de destino, puede seguir una ruta diferente a través de la red. Del otro lado (el programa cliente en nuestro ordenador), TCP reconstruye los paquetes individuales y espera hasta que hayan llegado todos para presentárnoslos como un solo fichero.

 **IP.** Se encarga de repartir los paquetes de información enviados entre el ordenador local y los ordenadores remotos. Esto lo hace etiquetando los paquetes con una serie de información, entre la que cabe destacar las direcciones IP de los dos ordenadores. Basándose en esta información, IP garantiza que los datos se encaminarán al destino correcto. Los paquetes recorrerán la red hasta su destino (que puede estar en el otro extremo del planeta) por el camino más corto posible gracias a unos dispositivos denominados *encaminadores* o routers.

Protocolos a Nivel de Aplicación

Aquí tenemos los protocolos asociados a los distintos servicios de Internet, como FTP, Telnet, Gopher, HTTP, etc. Estos protocolos son visibles para el usuario en alguna medida. Por ejemplo, el protocolo FTP (File Transfer Protocol) es visible para el usuario. El usuario solicita una conexión a otro ordenador para transferir un fichero, la conexión se establece, y comienza la transferencia. Durante dicha transferencia, es visible parte del intercambio entre la máquina

del usuario y la máquina remota (mensajes de error y de estado de la transferencia, como por ejemplo cuantos bytes del fichero se han transferido en un momento dado).

Breve Historia del Protocolo TCP/IP

A principios de los años 60, varios investigadores intentaban encontrar una forma de compartir recursos informáticos de una forma más eficiente. En 1961, Leonard Klienrock introduce el concepto de *Conmutación de Paquetes* (*Packet Switching*, en inglés). La idea era que la comunicación entre ordenadores fuese dividida en *paquetes*. Cada paquete debería contener la dirección de destino y podría encontrar su propio camino a través de la red.

Como ya comentamos en el capítulo anterior, en 1969 la Agencia de Proyectos de Investigación Avanzada (Defense Advanced Research Projects Agency o DARPA) del Ejército de los EEUU desarrolla la ARPAnet. La finalidad principal de esta red era la capacidad de resistir un ataque nuclear de la URSS para lo que se pensó en una administración descentralizada. De este modo, si algunos ordenadores eran destruidos, la red seguiría funcionando. Aunque dicha red funcionaba bien, estaba sujeta a algunas caídas periódicas del sistema. De este modo, la expansión a largo plazo de esta red podría resultar difícil y costosa. Se inició entonces una búsqueda de un conjunto de protocolos más fiables para la misma. Dicha búsqueda finalizó, a mediados de los 70, con el desarrollo de TCP/IP.

TCP/IP tenía (y tiene) ventajas significativas respecto a otros protocolos. Por ejemplo, consume pocos recursos de red. Además, podía ser implementado a un coste mucho menor que otras opciones disponibles entonces. Gracias a estos aspectos, TCP/IP comenzó a hacerse popular. En 1983, TCP/IP se integró en la versión 4.2 del sistema operativo UNIX de Berkeley y la integración en versiones comerciales de UNIX vino pronto. Así es como TCP/IP se convirtió en el estándar de Internet.

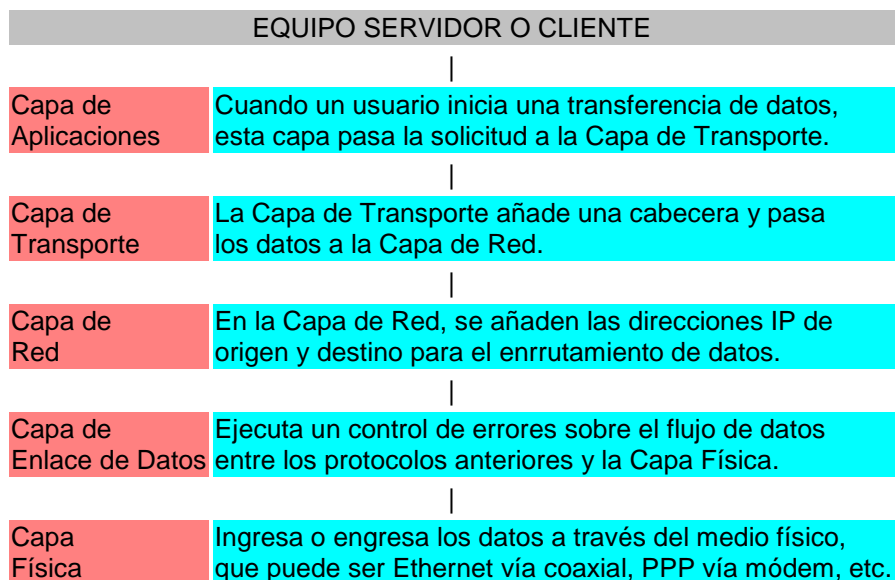
En la actualidad, TCP/IP se usa para muchos propósitos, no solo en Internet. Por ejemplo, a menudo se diseñan *intranets* usando TCP/IP. En tales entornos, TCP/IP ofrece ventajas significativas sobre otros protocolos de red. Una de tales ventajas es que trabaja sobre una gran variedad de hardware y sistemas operativos. De este modo puede crearse fácilmente una red heterogénea usando este protocolo. Dicha red puede contener estaciones Mac, PC compatibles, estaciones Sun, servidores Novell, etc. Todos estos elementos pueden comunicarse usando la misma suite de protocolos TCP/IP. La siguiente tabla muestra una lista de plataformas que soportan TCP/IP:

<i>Plataforma</i>	<i>Soporte de TCP/IP</i>
UNIX	Nativo
DOS	Piper/IP por Ipswitch
Windows	TCPMAN por Trumpet Software
Windows 95	Nativo
Windows NT	Nativo
Macintosh	MacTCP u OpenTransport (Sys 7.5+)
OS/2	Nativo
AS/400 OS/400	Nativo

Las plataformas que no soportan TCP/IP nativamente lo implementan usando programas TCP/IP de terceras partes, como puede apreciarse en la tabla anterior.

Cómo Trabaja TCP/IP

TCP/IP opera a través del uso de una pila. Dicha pila es la suma total de todos los protocolos necesarios para completar una transferencia de datos entre dos máquinas (así como el camino que siguen los datos para dejar una máquina o entrar en la otra). La pila está dividida en capas, como se ilustra en la figura siguiente:



Después de que los datos han pasado a través del proceso ilustrado en la figura anterior, viajan a su destino en otra máquina de la red. Allí, el proceso se ejecuta al revés (los datos entran por la capa física y recorren la pila hacia arriba). Cada capa de la pila puede enviar y recibir datos desde la capa adyacente. Cada capa está también asociada con múltiples protocolos que trabajan sobre los datos.

El Programa Inetd y los Puertos

Cada vez que una máquina solicita una conexión a otra, especifica una dirección particular. En general, esta dirección será la dirección IP Internet de dicha máquina. Pero hablando con más detalle, la máquina solicitante especificará también la aplicación que está intentando alcanzar dicho destino. Esto involucra a dos elementos: un programa llamado *inetd* y un sistema basado en *puertos*.

Inetd. Inetd pertenece a un grupo de programas llamados TSR (*Terminate and stay resident*). Dichos programas siempre están en ejecución, a la espera de que se produzca algún suceso determinado en el sistema. Cuando dicho suceso ocurre, el TSR lleva a cabo la tarea para la que está programado.

En el caso de *inetd*, su finalidad es estar a la espera de que se produzca alguna solicitud de conexión del exterior. Cuando esto ocurre, *inetd* evalúa dicha solicitud determinando que servicio está solicitando la máquina remota y le pasa el control a dicho servicio. Por ejemplo, si la máquina remota solicita una página web, le pasará la solicitud al proceso del servidor Web.

En general, *inetd* es iniciado al arrancar el sistema y permanece residente (a la escucha) hasta que apagamos el equipo o hasta que el operador del sistema finaliza expresamente dicho proceso.

Puertos. La mayoría de las aplicaciones TCP/IP tienen una filosofía de cliente-servidor. Cuando se recibe una solicitud de conexión, *inetd* inicia un programa servidor que se encargará de comunicarse con la máquina cliente. Para facilitar este proceso, a cada aplicación (FTP o

Telnet, por ejemplo) se le asigna una única dirección. Dicha dirección se llama *puerto*. Cuando se produce una solicitud de conexión a dicho puerto, se ejecutará la aplicación correspondiente.

Aunque la asignación de puertos a los diferentes servicios es de libre elección para los administradores de sistema, existe un estándar en este sentido que es conveniente seguir. La tabla que se muestra a continuación presenta un listado de algunas asignaciones estándar:

<i>Servicio o Aplicación</i>	<i>Puerto</i>
File Transfer Protocol (FTP)	21
Telnet	23
Simple Mail Transfer Protocol (SMTP)	25
Gopher	70
Finger	79
Hypertext Transfer Protocol (HTTP)	80
Network News Transfer Protocol (NNTP)	119

Números IP

En el capítulo anterior vimos que una dirección IP consistía en cuatro números separados por puntos, estando cada uno de ellos en el rango de 0 a 254. Por ejemplo, una dirección IP válida sería 193.146.85.34. Cada uno de los números decimales representa una cadena de ocho dígitos binarios. De este modo, la dirección anterior sería realmente la cadena de ceros y unos:

11000001.10010010.01010101.00100010

NOTA: Podemos usar la Calculadora de Windows 95 para realizar las conversiones de binario-decimal y viceversa.

La versión actual del protocolo IP (la versión 4 o IPv4) define de esta forma direcciones de 32 bits, lo que quiere decir que hay 2^{32} (4.294.967.296) direcciones IPv4 disponibles. Esto parece un gran número, pero la apertura de nuevos mercados y el hecho de que un porcentaje significativo de la población mundial sea candidato a tener una dirección IP, hacen que el número finito de direcciones pueda agotarse eventualmente. Este problema se ve agravado por el hecho de que parte del espacio de direccionamiento está mal asignado y no puede usarse a su máximo potencial.

Por otra parte, el gran crecimiento de Internet en los últimos años ha creado también dificultades para encaminar el tráfico entre el número cada vez mayor de redes que la componen. Esto ha creado un crecimiento exponencial del tamaño de las tablas de encaminamiento que se hacen cada vez más difíciles de sostener.

Los problemas comentados se han solucionado en parte hasta la fecha introduciendo progresivos niveles de jerarquía en el espacio de direcciones IP, que pasamos a comentar en los siguientes apartados. No obstante, la solución a largo plazo de estos problemas pasa por desarrollar la próxima generación del protocolo IP (IPng o IPv6) que puede alterar algunos de nuestros conceptos fundamentales acerca de Internet.

Clasificación del Espacio de Direcciones

Cuando el protocolo IP se estandarizó en 1981, la especificación requería que a cada sistema conectado a Internet se le asignase una única dirección IP de 32 bits. A algunos sistemas,

como los routers, que tienen interfaces a más de una red se les debía asignar una única dirección IP para cada interfaz de red. La primera parte de una dirección IP identifica la red a la que pertenece el host, mientras que la segunda identifica al propio host. Por ejemplo, en la dirección 135.146.91.26 tendríamos:

Prefijo de Red	Número de Host
135.146	91.26

Esto crea una jerarquía del direccionamiento a dos niveles. Recordemos que la dirección es realmente una cadena de 32 dígitos binarios, en la que en el ejemplo anterior hemos usado los 24 primeros para identificar la red y los 8 últimos para identificar el host.

Clases Primarias de Direcciones. Con la finalidad de proveer la flexibilidad necesaria para soportar redes de distinto tamaño, los diseñadores decidieron que el espacio de direcciones debería ser dividido en tres clases diferentes: Clase A, Clase B y Clase C. Cada clase fija el lugar que separa la dirección de red de la de host en la cadena de 32 bits.

Una de las características fundamentales de este sistema de clasificación es que cada dirección contiene una clave que identifica el punto de división entre el prefijo de red y el número de host. Por ejemplo, si los dos primeros bits de la dirección son 1-0 el punto estará entre los bits 15 y 16.

Redes Clase A (/8). Cada dirección IP en una red de clase A posee un prefijo de red de 8 bits (con el primer bit puesto a 0 y un número de red de 7 bits), seguido por un número de host de 24 bits.

El posible definir un máximo de 126 (2^7-2) redes de este tipo y cada red /8 soporta un máximo de 16.777.214 ($2^{24}-2$) hosts. Obsérvese que hemos restado dos números de red y dos números de host. Estos números no pueden ser asignados ni a ninguna red ni a ningún host y son usados para propósitos especiales. Por ejemplo, el número de host "todos 0" identifica a la propia red a la que "pertenece".

Traduciendo los números binarios a notación decimal, tendríamos el siguiente rango de direcciones para la red /8 o clase A:

1.xxx.xxx.xxx hasta 126.xxx.xxx.xxx

Redes Clase B (/16). Tienen un prefijo de red de 16 bits (con los dos primeros puestos a 1-0 y un número de red de 14 bits), seguidos por un número de host de 16 bits. Esto nos da un máximo de 16.384 (2^{14}) redes de este tipo, pudiéndose definir en cada una de ellas hasta 65.534 ($2^{16}-2$) hosts.

Traduciendo los números binarios a notación decimal, tendríamos el siguiente rango de direcciones para la red /16 o clase B:

128.0.xxx.xxx hasta 191.255.xxx.xxx

Redes Clase C (/24). Cada dirección de red clase C tiene un prefijo de red de 24 bits (siendo los tres primeros 1-1-0 con un número de red de 21 bits), seguidos por un número de host de 8 bits. Tenemos así 2.097.152 (2^{21}) redes posibles con un máximo de 254 (2^8-2) host por red.

El rango de direcciones en notación decimal para las redes clase C sería:

192.0.0.xxx hasta 223.255.255.xxx

Subredes

En 1985 se define el concepto de subred, o división de un número de red Clase A, B o C, en partes más pequeñas. Dicho concepto es introducido para subsanar algunos de los problemas que estaban empezando a producirse con la clasificación del direccionamiento de dos niveles jerárquicos.

- Las tablas de enrutamiento de Internet estaban empezando a crecer.
- Los administradores locales necesitaban solicitar otro número de red de Internet antes de que una nueva red se pudiese instalar en su empresa.

Ambos problemas fueron abordados añadiendo otro nivel de jerarquía, creándose una jerarquía a tres niveles en la estructura del direccionamiento IP. La idea consistió en dividir la parte dedicada al número de host en dos partes: el número de subred y el número de host en esa subred:

Jerarquía a dos Niveles

Prefijo de Red	Número de Host
135.146	91.26

Jerarquía a tres Niveles

Prefijo de Red	Número de Subred	Número de Host
135.146	91	26

Este sistema aborda el problema del crecimiento de las tablas de enrutamiento, asegurando que la división de una red en subredes nunca es visible fuera de la red privada de una organización. Los routers dentro de la organización privada necesitan diferenciar entre las subredes individuales, pero en lo que se refiere a los routers de Internet, todas las subredes de una organización están agrupadas en una sola entrada de la tabla de rutas. Esto permite al administrador local introducir la complejidad que desee en la red privada, sin afectar al tamaño de las tablas de rutas de Internet.

Por otra parte, sólo hará falta asignar a la organización un único número de red (de las clases A,B o C) o como mucho unos pocos. La propia organización se encargará entonces de asignar distintos números de subred para cada una de sus redes internas. Esto evita en la medida de lo posible el agotamiento de los números IP disponibles.

Máscara de Subred

Prefijo de Red extendido. Los routers de Internet usan solamente el prefijo de red de la dirección de destino para encaminar el tráfico hacia un entorno con subredes. Los routers dentro del entorno con subredes usan el prefijo de red extendido para encaminar el tráfico entre las subredes. El prefijo de red extendido está compuesto por el prefijo de red y el número de subred:

Prefijo de Red Extendido		
Prefijo de Red	Número de Subred	Número de Host

El prefijo de red extendido se identifica a través de la *máscara de subred*. Por ejemplo, si consideramos la red clase B 135.146.0.0 y queremos usar el tercer octeto completo para representar el número de subred, deberemos especificar la máscara de subred 255.255.255.0

Entre los bits en la máscara de subred y la dirección de Internet existe una correspondencia uno a uno. Los bits de la máscara de subred están a 1 si el sistema que examina la dirección debe tratar los bits correspondientes en la dirección IP como parte del prefijo de red extendido. Los bits de la máscara están a 0 si el sistema debe considerar los bits como parte del número de host. Esto se ilustra en la siguiente figura:

		prefijo de red		nº subred	nº host
Dirección IP	135.146.91.26	10000111	10010010	01011011	00011010
Máscara de Subred	255.255.255.0	11111111	11111111	11111111	00000000
		prefijo de red extendido			

En lo que sigue nos referiremos a la *longitud del prefijo de red extendido* más que a la máscara de subred, aunque indican lo mismo. La longitud del prefijo es igual al número de bits a 1 contiguos en la máscara de subred. De este modo, la dirección 135.146.91.26 con una máscara de subred 255.255.255.0 podrá expresarse también de la forma 135.146.91.26/24, lo que resulta más compacto y fácil de entender.

Caso práctico

Pero veamos un caso práctico para comprender mejor esta clasificación con tres niveles jerárquicos. A una organización se le ha asignado el número de red 193.1.1.0/24 (esto es, una clase C) y dicha organización necesita definir seis subredes. La subred más grande puede contener un máximo de 25 hosts.

Primer paso (definir la máscara de subred). Lo primero que debemos hacer es determinar el número de bits necesarios para definir las 6 subredes. Dada la naturaleza del sistema de numeración binario esto sólo puede hacerse tomando múltiplos de 2. Así que cogeremos $2^3=8$ y podemos dejar las 2 subredes restantes previendo un eventual crecimiento de nuestra red.

Como $8=2^3$, se necesitan 3 bits para numerar las 8 subredes. Como estamos hablando de una clase C (/24), sumamos 3 y nuestro prefijo de red extendido será /27 que en decimal nos daría la máscara 255.255.255.224. Esto se ilustra en la figura siguiente:

	prefijo de red			bits nº subr	bits nº host
193.1.1.0/24=	11000001	00000001	00000001	000	00000
prefijo de red extendido					
255.255.255.224=	11111111	11111111	11111111	111	00000
27 bits					

NOTA: Para no desanimarse, podemos coger la calculadora y hacer la conversión de 11100000 a decimal, que dará justamente 224.

Segundo paso (definir los números de subred). Las ocho subredes se numerarán de 0 a 7. Lo único que tenemos que hacer es colocar la representación binaria de dichos números en el campo *bits nº subred* de la primera fila de la figura anterior, y luego traducir las direcciones binarias a decimal. Quedaría lo siguiente:

Red Base: 11000001.00000001.00000001.00000000=193.1.1.0/24
 Subred 0: 11000001.00000001.00000001.**000**00000=193.1.1.0/27
 Subred 1: 11000001.00000001.00000001.**001**00000=193.1.1.32/27
 Subred 2: 11000001.00000001.00000001.**010**00000=193.1.1.64/27
 Subred 3: 11000001.00000001.00000001.**011**00000=193.1.1.96/27
 Subred 4: 11000001.00000001.00000001.**100**00000=193.1.1.128/27
 Subred 5: 11000001.00000001.00000001.**101**00000=193.1.1.160/27

Subred 6: 11000001.00000001.00000001.**11000000**=193.1.1.192/27

Subred 7: 11000001.00000001.00000001.**11100000**=193.1.1.224/27

Tercer paso (definir los números de host). En nuestro ejemplo, disponemos de 5 bits en el campo *bits nº host* de cada dirección de subred. Esto nos da un bloque de 30 ($=2^5-2$) direcciones de host posibles, que cubre los 25 que se prevén como máximo. Obsérvese que restamos 2 pues las direcciones de host todos 0 (esta subred) o todos 1 (broadcast) no pueden usarse. Los host de cada subred se numeran del 0 al 30. Para definir la dirección asignada al host n de una subred dada, colocaremos la representación binaria de n en el campo *bits nº host* y luego traduciremos la dirección completa a notación decimal. Por ejemplo, para la subred 2 quedaría:

Subred 2: 11000001.00000001.00000001.010**00000**=193.1.1.64/24

Host 1: 11000001.00000001.00000001.010**00001**=193.1.1.64/27

Host 2: 11000001.00000001.00000001.010**00010**=193.1.1.65/27

Host 3: 11000001.00000001.00000001.010**00011**=193.1.1.66/27

.
. .
.

Host 29: 11000001.00000001.00000001.010**11101**=193.1.1.93/27

Host 30: 11000001.00000001.00000001.010**11110**=193.1.1.94/27



En el ejemplo anterior, la parte inicial de cada dirección identifica el prefijo de red extendido, mientras que los dígitos en negrita indican el campo de 5 bits número de host.

DNS

Como ya comentamos en el capítulo dedicado a Internet, el DNS (Domain Name System, o Sistema de Nombres de Dominio) es un sistema que hace corresponder a la dirección IP de cada host de Internet un único nombre de dominio, para que podamos acceder a dicho host con mayor facilidad. Además, veíamos que la estructura de dichos nombres es jerárquica, algo similar a *Nombre_del_host.Subsubdominio.Subdominio.Dominio*. Estudiaremos ahora con más detalle este tema. Comenzamos explicando algunos conceptos previos que nos servirán para comprender mejor el tema.

Nombres de equipos NetBIOS y DNS

En Windows 95 pueden utilizarse dos tipos de nombres para los equipos:

-  El nombre NetBIOS, que consta de una única parte y que será el que indiquemos en la casilla Identificación dentro del cuadro de diálogo Red en el Panel de control.
-  El nombre DNS, que consta de dos partes: un nombre de host y un nombre de dominio, que juntos forman el nombre completo de dominio (FQDN o Fully Qualified Domain Name). Este nombre se puede indicar en el cuadro de diálogo Propiedades de TCP/IP accesible también a través del cuadro de diálogo Red.

Resolución de nombres

En las redes TCP/IP, los ordenadores se identifican a través de su dirección IP. Sin embargo, a los usuarios les resulta más fácil usar nombres para los ordenadores en vez de números, por lo que se hace necesario establecer un mecanismo que resuelva nombres en direcciones IP cuando se soliciten conexiones dando los nombres de los ordenadores remotos. Esto se conoce como un sistema de resolución de nombres. En las redes Windows existen diversos sistemas de resolución de nombres disponibles:

Resolución de nombres por difusión. Cuando un equipo se conecta a la red, realizará difusiones a nivel IP para registrar su nombre NetBIOS anunciándolo en la red. Cada equipo en el área de difusión es responsable de cancelar cualquier intento de registrar un nombre duplicado. Uno de los problemas existentes en este sistema es que, si la red es grande, se sobrecargará de difusiones. No obstante, resultará el adecuado en nuestra Intranet para las conexiones internas.

Servicio de nombres Internet de Windows (WINS, Windows Internet Naming Service).

Utiliza una base de datos dinámica que hace corresponder nombres de equipos NetBIOS con direcciones IP. Dicha base de datos reside en un servidor WINS (que será una máquina con Windows NT server). WINS reduce el uso de la resolución por difusión y permite a los usuarios localizar fácilmente sistemas en redes remotas.

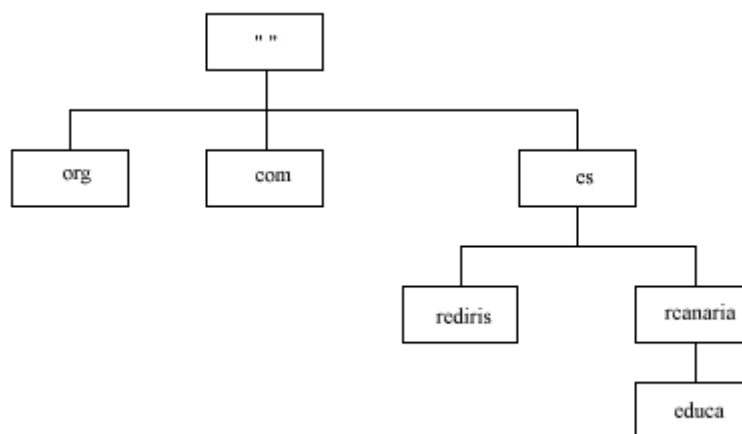
Resolución de nombres usando el Sistema de nombres de dominio (DNS). DNS permite resolver nombres DNS a direcciones IP cuando un ordenador se conecta a ordenadores remotos fuera de la red local (por ejemplo, a nodos de Internet). Necesita un servidor de nombres DNS. En nuestro caso dicho servidor será el de Red Canaria, al cual accedemos a través de nuestro router que actuará como puerta de enlace o gateway para cada estación de nuestra red local. Para más detalles sobre DNS ver el apartado siguiente.

Ficheros LMHOSTS y HOSTS. Ambos ficheros se utilizan en ordenadores locales para enumerar direcciones IP conocidas de ordenadores remotos junto con sus nombres de equipo. El fichero LMHOSTS especifica el nombre NetBIOS del ordenador remoto y su dirección IP. El fichero HOST especifica el nombre DNS y la dirección IP. Pueden considerarse como equivalentes locales a los servicios WINS y DNS y pueden usarse para resolver nombres de ordenadores remotos a direcciones IP cuando los servicios anteriores no están disponibles. En nuestro caso, usaremos un fichero HOSTS en cada una de nuestras estaciones para indicar el nombre y la dirección IP de nuestro servidor web interno (Servweb), ya que al tener el DNS activado en dichas estaciones (para acceder a Internet), cuando no estemos conectados dicho DNS no estará operativo con la consiguiente ralentización en la resolución del nombre del servidor web interno.

Sistema de nombres de dominio (DNS o Domain Name System)

El DNS es una base de datos distribuida que proporciona un sistema de nomenclatura jerárquico para indentificar hosts en Internet.

Espacio de nombres de dominio. La base de datos DNS tiene una estructura en árbol que se llama *espacio de nombres de dominio*. Cada dominio (o nodo en el árbol) tiene un nombre y puede contener subdominios. El *nombre de dominio* identifica la posición del dominio en el árbol respecto a su dominio principal, utilizándose puntos para separar los nombres de los nodos. Por ejemplo, el nombre de dominio *rcanaria.es* se refiere al subdominio *rcanaria* perteneciente al dominio principal *es*.



Dominios de primer nivel. Los dominios del nivel superior en la base de datos DNS pueden ser genéricos (com, org, edu, etc.) o territoriales (uk, es, etc.). Para obtener un listado completo, consultar el capítulo 1. La administración de dichos dominios se lleva a cabo por un organismo llamado InterNIC.

Dominios de niveles inferiores y zonas. Por debajo del primer nivel, InterNIC delega en otras organizaciones la administración del espacio de nombres de dominio. El árbol DNS queda dividido en zonas, donde cada zona es una unidad administrativa independiente. Las zonas pueden ser un único dominio o un dominio dividido en subdominios. Por ejemplo, el dominio *rcanaria* sería una zona administrativa del árbol DNS.

Nombres de dominio completos. Un nombre de dominio completo (FQDN o Fully Qualified Domain Name) se forma siguiendo la ruta desde la parte inferior del árbol DNS (nombre de host) hasta la raíz de dicho árbol. En el FQDN el nombre de cada nodo es separado por un punto. Un ejemplo de FQDN sería *www.educa.rcanaria.es*.

Servidores de nombres y resolvers. Los servidores DNS o servidores de nombre contienen información de una parte de la base de datos DNS (zona) para satisfacer las demandas de los clientes DNS. Cuando un ordenador cliente (*resolver*) solicita una conexión a un ordenador remoto de Internet a través de su FQDN, el servidor de nombres buscará el FQDN en su porción de la base de datos DNS. Si está ahí, satisfará de inmediato la demanda del resolver. En caso contrario, consultará a otros servidores de nombres para intentar responder a la consulta.